Subpart 1852.2—Texts of Provisions and Clauses

1852.203–70 Display of Inspector General Hotline Posters.

As prescribed in 1803.7001, insert the following clause:

DISPLAY OF INSPECTOR GENERAL HOTLINE POSTERS (JUN 2001)

(a) The Contractor shall display prominently in common work areas within business segments performing work under this contract, Inspector General Hotline Posters available under paragraph (b) of this clause.

(b) Inspector General Hotline Posters may be obtained from NASA Office of Inspector General, Code W, Washington, DC, 20546–0001, (202) 358–1220.

[66 FR 29727, June 1, 2001]

1852.204–75 Security classification requirements.

As prescribed in 1804.404–70, insert the following clause:

SECURITY CLASSIFICATION REQUIREMENTS (SEP 1989)

Performance under this contract will involve access to and/or generation of classified information, work in a security area, or both, up to the level of _____ [insert the applicable security clearance level]. See Federal Acquisition Regulation clause 52.204–2 in this contract and DD Form 254, Contract Security Classification Specification, Attachment _____ [Insert the attachment number of the DD Form 254].

(End of clause)

[61 FR 40548, Aug. 5, 1996]

1852.204–76 Security requirements for unclassified information technology resources.

As prescribed in 1804.470–4(a), insert the following clause:

SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (MONTH YEAR)

(a) The contractor shall protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources and protect NASA Electronic Information from unauthorized disclosure.

(b) This clause is applicable to all NASA contractors and sub-contractors that process, manage, access, or store unclassified electronic information, to include Sensitive But Unclassified (SBU) information, for NASA in support of NASA's missions, programs, projects and/or institutional requirements. Applicable requirements, regulations, policies, and guidelines are identified in the Applicable Documents List (ADL) provided as an attachment to the contract. The documents listed in the ADL can be found at: *http://www.nasa.gov/offices/ocio/itsecurity/index.html*. For policy information considered sensitive, the documents will be identified as such in the ADL and made available through the Contracting Officer.

(c) Definitions.

(1) IT resources means any hardware or software or interconnected system or subsystem of equipment, that is used to process, manage, access, or store electronic information.

(2) NASA Electronic Information is any data (as defined in the Rights in Data clause of this contract) or information (including information incidental to contract administration, such as financial, administrative, cost or pricing, or management information) that is processed, managed, accessed or stored on an IT system(s) in the performance of a NASA contract.

(3) IT Security Management Plan—This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. Unlike the IT security plan, which addresses the IT system, the IT Security Management Plan addresses how the contractor will manage personnel and processes associated with IT Security on the instant contract.

(4) IT Security Plan—this is a FISMA requirement; see the ADL for applicable requirements. The IT Security Plan is specific to the IT System and not the contract. Within 30 days after award, the contractor shall develop and deliver an IT Security Management Plan to the Contracting Officer; the approval authority will be included in the ADL. All contractor personnel requiring physical or logical access to NASA IT resources must complete NASA's annual IT Security Awareness training. Refer to the IT Training policy located in the IT Security Web site at *https://itsecurity.nasa.gov/policies/index.html*.

(d) The contractor shall afford Government access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry out a program of IT inspection (to include vulnerability testing), investigation and audit to safeguard against threats and hazards to the integrity, availability, and